# 基于 $d$ 维纠缠交换的 $(t, n)$ 门限量子秘密共享 *

宋秀丽†，徐建坤，周道洋

(重庆邮电大学 网络信息安全技术重庆市重点工程实验室，重庆 400065)

**摘　要：**以 $d$ 维纠缠交换为技术手段，提出了一个 $(t, n)$ 门限量子秘密共享方案。该方案执行 $t$ 次 $d$ 维纠缠交换，秘密影子聚合于重建者的 $V_1$ 粒子中。重建者测量该粒子，可重建出共享的秘密。安全性分析可知，提出的方案，能抵抗截获-重发攻击、纠缠-测量攻击、合谋攻击和伪造攻击。性能比较分析表明，相比较于其他现有类似量子秘密共享方案，提出的方案具有更好的灵活性、实用性和普适性。而且总的计算和测量所花费的开销是最低的。

**关键词：**$d$ 维 Hilbert 空间；$(t, n)$ 门限；纠缠交换；量子秘密共享；投影测量

**中图分类号：**TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.12.0758

# $(t, n)$ threshold quantum secret sharing based on $d$-dimensional entanglement swapping

Song Xiuli†, Xu Jiankun, Zhou Daoyang

(*Chongqing Key Laboratory of Network Information Security Technology*, *Chongqing University of Posts & Telecommunications*, *Chongqing* 400065, *China*)

**Abstract:** This paper proposed a $(t, n)$ threshold quantum secret sharing scheme by means of $d$-dimensional entanglement swapping. The proposed scheme has executed $t$ times of $d$-dimensional entanglement swapping, which aggregates secret shadows into $V_1$ particle of the reconstructor. Finally, the reconstructor measures this particle to reconstruct the original secret. Security analysis shows that the proposed scheme can resist intercept-resend, entangle-measure, collusion and forgery attacks. By comparison with other similar schemes in performance, the proposed scheme is more flexible, practical and universal. In addition, its total overheads of computation and measurement are lowest in current similar quantum secret sharing schemes.

**Key words:** $d$-dimensional Hilbert space; $(t, n)$ threshold; entanglement swapping; quantum secret sharing; projection measurement



## 0　引言

在某些场合，为了让多人承担保护秘密消息的风险，或者加强对某个秘密消息的保密强度，需要多个参与者共同参与保护这个秘密消息。解决这个问题常用的技术是经典秘密共享。经典秘密共享将一个秘密消息拆分成若干个秘密份额，并将这些秘密份额分发给若干个参与者，由这些参与者共同管理，只有若干个参与者一起合作才能恢复出秘密消息。由于经典秘密共享很难克服秘密份额在经典公共信道传输过程中被窃听的问题，于是 1999 年，Hillery 等人[1]将经典秘密共享扩展到量子世界中。在该方案中，秘密份额可在量子信道中分发给参与者，克服了经典秘密共享的安全缺陷。

此后，许多量子秘密共享方案[2~20]被提出。在这些方案中，文献[2~7,11,13~16,19]是 $(n,n)$ 的量子秘密共享方案。它们必须 $n$ 个参与者同时到场，一起合作才能恢复出秘密，现实生活中，有可能一个或多个参与者生病、出差等特殊情况不能到场，此时，共享的秘密无法恢复。文献[2~5,8~9,11~12,14~20]是 2 维量子秘密共享方案，它们制备的量子态都处在 2 维希尔伯特空间，如果将这些方案置于比 2 更高维的量子通信环境中，它们无法直接运行，需要进行维度的转换。文献[8~9,12,17~18,20]是 $(t,n)$ 的量子秘密共享方案，只需要 $t$ 个或大于 $t$ 个参与者就能恢复出秘密，但它们制备的量子态是处在 2 维希尔伯特空间。文献[6,7,13]是 $d$ $(d>2)$ 维量子秘密共享方案，但它们是 $(n,n)$ 门限。文献[5,13]在秘密重构阶段应用纠缠交换实现隐形传输，份额没有量子信道中传输，但文献[5]是 2 维的 $(3,3)$ 门限方案，文献[13]是 $d$ 维的 $(n,n)$ 门限方案。

为了突破 Hilbert 空间 2 维度的局限性，解决某些参与者无法到场重建共享秘密的问题，本文提出了一种 $d$ 维 $(t,n)$ 门限量子秘密共享方案，克服了上述方案的局限性。该方案将秘密影子加入到投影测量算子的相位中，当选择的 $t$ 个参与者都执行

---

**基金项目：**国家自然科学基金资助项目（61772098，61772099）；重庆市科学技术委员会基础科学与前沿技术项目（cstc2016jcyjA0571）；重庆邮电大学高端人才培养项目（BYJS2016002）

**作者简介：**宋秀丽（1972-），女（通信作者），副教授，硕导，主要研究方向为量子保密通信（songxl@cqupt.edu.cn）；徐建坤（1993-），男，湖北孝感人，硕士研究生，主要研究方向为量子保密通信；周道洋（1993-），男，硕士研究生，主要研究方向为量子保密通信.

完投影测量，复合系统发生 $t$ 次 $d$ 维纠缠交换，秘密影子聚合于重建者 $Bob_1$ 的 $V_1$ 粒子中，测量该粒子，恢复出共享的秘密消息。与上述方案相比，提出的方案的主要贡献体现在：a)它制备的量子态处在 $d$ $(d>2)$ 维希尔伯特空间中，当量子环境是自由空间时，它比 2 维量子秘密共享具有更好的普适性;b)它以 $t$ $(t\le n)$ 为门限值，与 $(n,n)$ 门限量子秘密共享相比，具有更好的灵活性和实用性;c)它在秘密重构阶段使用纠缠交换实现份额隐形传输，这些份额并没有在量子信道中传输，比那些将经典份额或量子份额在量子信道中传输的方案，具有更高的安全性。

## 1 提出的 $d$ 维 $(t,n)$ 门限量子秘密共享方案

在提出的方案中，Alice 是受信的秘密分发者，$B_n=\{Bob_1,Bob_2,\cdots,Bob_n\}$ 是 $n$ 个参与者的集合，Alice 从其中选择 $Bob_1$ 作为可信任的重建者。$Bob_1$ 的职责是从 $n$ 个参与者持有的份额中收集任意 $t$ 个份额，然后重建出原始的秘密信息。提出的 $d$ 维 $(t,n)$ 门限量子秘密共享方案由四个阶段组成：份额分发阶段，粒子制备阶段，纠缠交换阶段，秘密重建阶段。

### 1.1 份额分发阶段

本阶段，受信的秘密分发者 Alice 生成 $n$ 个秘密份额发送给 $n$ 个参与者，并将共享秘密的 hash 值发给重建者 $Bob_1$。

a）Alice 寻找一个合适素数 $d$，满足 $n\le d\le 2n$（因为需要 $n$ 个不同的非零整数，再加上 $2n$ 维空间的限制是对粒子制备的复杂度的限制）。并在 $GF(d)$ 域上随机生成一个 $t-1$ 次多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$，其中 $(a_0,a_1,a_2,\cdots,a_{t-1})\in Z_d^t$，$a_0$ 是秘密消息。Alice 再选择 $n$ 个互不相等且非零整数 $x_i(i=1,2,\cdots,n)$，并公布 $x_i$。她以 $x_i$ 为参数计算 $n$ 个秘密份额 $f(x_i)$，并通过安全的量子信道将它们发送给 $n$ 个参与者，每个参与者 $Bob_i$ 手中持有一个秘密份额 $f(x_i)$。虽然每个秘密份额 $f(x_i)$ 为参与者 $Bob_i$ 本地所持有，但是其中任意 $t$ 个秘密份额 $\{f(x_1),f(x_2),\cdots,f(x_t)\}$ 在 $GF(d)$ 域上满足下面关系

$$a_0=f(0)=\sum_{r=1}^{t}f(x_r)\prod_{1\le b\le t,b\ne r}\frac{x_b}{x_b-x_r}\bmod d\text{。}\tag{1}$$

b)Alice 使用公开的 hash 算法（如 SHA-256），计算 $hash(a_0)$，也通过安全的量子信道把它发送给参与者 $Bob_1$。

### 1.2 粒子制备阶段

在 $n$ 个参与者中，假定临时到场的参与者集合为 $B_t=\{Bob_1,Bob_2,\cdots,Bob_t\}$。其中，$Bob_1$ 既是粒子的制备者，也是可信的重建者。粒子制备阶段步骤如下：

a）$Bob_1$ 制备 $t$ 个 $d$ 维单粒子 $\{|u_1\rangle_{U_1},|u_2\rangle_{U_2},\cdots,|u_t\rangle_{U_t}\}$，其中，$u_r$ 表示第 $r(r=1,2,\cdots,t)$ 粒子的取值，$U_r$ 表示第 $r(r=1,2,\cdots,t)$ 个粒子的标签。

b）$Bob_1$ 对 $U_1$ 粒子 $|u_1\rangle_{U_1}$ 作 $d$ 维哈达门变换 $H_d$，则 $t$ 个粒子 $\{|u_1\rangle_{U_1},|u_2\rangle_{U_2},\cdots,|u_t\rangle_{U_t}\}$ 组成了一个的复合系统态 $|\varphi_1\rangle$

$$\begin{aligned}|\varphi_1\rangle&=\left(H_d|u_1\rangle_{U_1}\right)|u_2\rangle_{U_2}|u_3\rangle_{U_3}\cdots|u_t\rangle_{U_t}\\&=\left(\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{qu_1}|q\rangle_{U_1}\right)|u_2\rangle_{U_2}|u_3\rangle_{U_3}\cdots|u_t\rangle_{U_t},\end{aligned}\tag{2}$$

其中 $\zeta=e^{2\pi i/d}$，$H_d=\frac{1}{\sqrt{d}}\sum_{q,u=0}^{d-1}\zeta^{qu}|q\rangle\langle u|$。

c）$Bob_1$ 以 $\left(H_d|u_1\rangle_{U_1}\right)$ 作为控制粒子，$|u_j\rangle_{U_j}$ $(j=2,3,\cdots,t)$ 作为目标粒子来进行 $d$ 维 $CNOT$ 门 $R_c$ 运算。经过 $(t-1)$ 个 $R_c$ 门运算后复合系统态 $|\varphi_1\rangle$ 演变为纠缠态 $|\varphi_2\rangle$，如图 1 所示[21]。

$$\begin{aligned}|\varphi_2\rangle&=\left(\bigotimes_{j=2}^{t}R_c\left(H_d|u_1\rangle_{U_1},|u_j\rangle_{U_j}\right)\right)|\varphi_1\rangle\\&=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{qu_1}|q\rangle_{U_1}|u_2+q\rangle_{U_2}|u_3+q\rangle_{U_3}\cdots|u_t+q\rangle_{U_t}\\&=|\psi_0(u_1,u_2,\cdots,u_t)\rangle_{U_1,U_2,\cdots,U_t},\end{aligned}\tag{3}$$

其中: $d$ 维 $CNOT$ 门 $R_c$ 满足条件：$R_c|u,q\rangle=|u,u+q\rangle$。

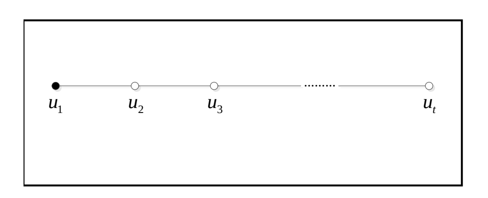



图 1 纠缠态 $|\psi_0(u_1,u_2,\cdots,u_t)\rangle_{U_1,U_2,\cdots,U_t}$

d）$Bob_1$ 通过授权的安全量子信道将纠缠态 $|\psi_0(u_1,u_2,\cdots,u_t)\rangle_{U_1,U_2,\cdots,U_t}$ 的第 $U_j(j=2,3,\cdots,t)$ 个粒子分别发送给相应的参与者 $Bob_j$。

e）当 $Bob_j(j=2,3,\cdots,t)$ 收到从 $Bob_1$ 发来的粒子后，集合 $B_t$ 中每个参与者 $Bob_r(r=1,2,\cdots,t)$ 取出其持有的秘密份额 $f(x_r)$，计算秘密影子 $s_r$：

$$s_r=f(x_r)\prod_{1\le b\le t,b\ne r}\frac{x_b}{x_b-x_r}\bmod d\text{。}\tag{4}$$

f）每个参与者 $Bob_r(r=1,2,\cdots,t)$ 制备一个 $d$ 维两粒子纠缠态 $|\psi(v_r,v_r')\rangle_{V_1,V_2}$，如图 2 所示。其中，

$$|\psi(v_r,v_r')\rangle_{V_r,V_r'}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{qv_r}|q\rangle_{V_r}|q+v_r'\rangle_{V_r'}\text{。}\tag{5}$$

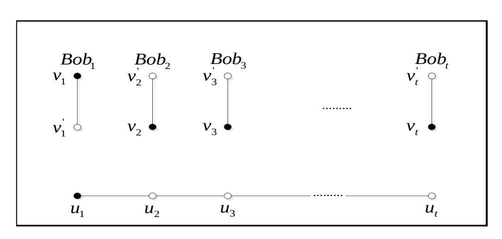



图 2 纠缠交换前的粒子分布图

### 1.3　纠缠交换阶段

参与者 $Bob_1$ 使用投影算子对自己持有的粒子 $\left(U_1,V_1^{'}\right)$ 进行投影测量，每个参与者 $Bob_j\left(j=2,3,\cdots,t\right)$ 依次使用投影算子对自己持有的粒子 $\left(V_r,U_r\right)$ 进行投影测量。当所有参与者 $B_t=\{Bob_1,Bob_2,\cdots,Bob_t\}$ 测量完毕，复合系统发生 $t$ 次 $d$ 维纠缠交换，秘密影子聚合于重建者 $Bob_1$ 的 $V_1$ 粒子相位中。具体步骤如下：

a）$Bob_1$ 使用投影算子 $\left|\psi\left(u_1-s_1,v_1^{'}\right)\right\rangle\left\langle\psi\left(u_1-s_1,v_1^{'}\right)\right|$ 对持有的粒子 $\left(U_1,V_1^{'}\right)$ 进行投影测量,测量的结果为 $\left|\psi\left(u_1-s_1,v_1^{'}\right)\right\rangle$。另外的 $t$ 个粒子 $\left(V_1,U_2,\cdots,U_t\right)$ 坍塌到 $\left|\psi_1\left(v_1+s_1,u_2,\cdots,u_t\right)\right\rangle_{V_1,U_2,\cdots,U_t}$ (为了描述方便，后续坍塌态都省略了前面的相位因子)。

这是因为由 $t$-纠缠粒子 $\left(U_1,U_2,\cdots,U_t\right)$ 和 2-纠缠粒子 $\left(V_1,V_1^{'}\right)$ 组成的混合系统 $\left|\Psi_1\right\rangle$ 为

$$\left|\Psi_1\right\rangle=\left|\psi\left(u_1,u_2,\cdots,u_t\right)\right\rangle_{U_1,U_2,\cdots,U_t}\otimes\left|\psi\left(v_1,v_1^{'}\right)\right\rangle_{V_1,V_1^{'}}$$

$$=\frac{1}{d}\sum_{k_1,l_1=0}^{d-1}\zeta^{-l_1k_1}\left|\psi\left(v_1+k_1,u_2-l_1,\cdots,u_t-l_1\right)\right\rangle_{V_1,U_2,\cdots,U_t}\otimes\left|\psi\left(u_1-k_1,v_1^{'}+l_1\right)\right\rangle_{U_1,V_1^{'}}。\tag{6}$$

当 $Bob_1$ 测量粒子 $\left(U_1,V_1^{'}\right)$ 之后，混合系统 $\left|\Psi_1\right\rangle$ 发生纠缠交换，如下图 3 所示。在式(6)右边的所有叠加项中，存在 $k_1=s_1,l_1=0$ 那一项为：

$$\frac{1}{d}\left|\psi\left(v_1+s_1,u_2,\cdots,u_t\right)\right\rangle_{V_1,U_2,\cdots,U_t}\otimes\left|\psi\left(u_1-s_1,v_1^{'}\right)\right\rangle_{U_1,V_1^{'}}$$

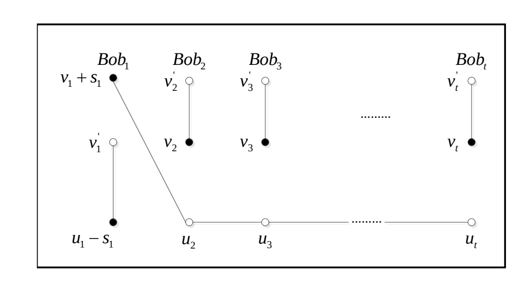



图 3　在粒子 $\left(U_1,V_1^{'}\right)$ 上投影测量之后的第一次纠缠交换

b）$Bob_2$ 使用投影算子 $\left|\psi\left(v_2-s_2,u_2\right)\right\rangle\left\langle\psi\left(v_2-s_2,u_2\right)\right|$ 对持有的粒子 $\left(V_2,U_2\right)$ 进行投影测量，测量的结果为 $\left|\psi\left(v_2-s_2,u_2\right)\right\rangle_{V_2,U_2}$。另外的 $t$ 个粒子（$V_1,V_2^{'},U_3,\cdots,U_t$）坍塌到 $\left|\psi_1\left(v_1+s_1+s_2,v_2^{'},u_3,\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},U_3,\cdots,U_t}$。由于有混合系统 $\left|\Psi_2\right\rangle$：

$$\left|\Psi_2\right\rangle=\left|\psi\left(v_1+s_1,u_2,\cdots,u_t\right)\right\rangle_{V_1,U_2,U_3,\cdots,U_t}\otimes\left|\psi\left(v_2,v_2^{'}\right)\right\rangle_{V_2,V_2^{'}}$$

$$=\frac{1}{d}\sum_{l_2,k_2=0}^{d-1}\zeta^{-l_2k_2}\left|\psi\left(v_1+s_1+k_2,v_2^{'}+l_2,u_3,\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},U_3,\cdots,U_t}\otimes\left|\psi\left(v_2-k_2,u_2-l_2\right)\right\rangle_{V_2,U_2}。\tag{7}$$

当 $Bob_2$ 测量粒子 $\left(V_2,U_2\right)$ 之后，混合系统 $\left|\Psi_2\right\rangle$ 发生纠缠交换。在式(7)右边的所有叠加项中，存在 $k_2=s_2,l_2=0$ 那一项为：

$$\frac{1}{d}\left|\psi\left(v_1+s_1+s_2,v_2^{'},u_3,\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},U_3,\cdots,U_t}\otimes\left|\psi\left(v_2-s_2,u_2\right)\right\rangle_{V_2,U_2}$$

c）其他参与者 $Bob_j\left(j=3,\cdots,t\right)$ 依次使用投影算子 $\left|\psi\left(v_j-s_j,u_j\right)\right\rangle\left\langle\psi\left(v_j-s_j,u_j\right)\right|$ 对持有的粒子 $\left(V_j,U_j\right)$ 进行投影测量，测量的结果为 $\left|\psi\left(v_j-s_j,u_j\right)\right\rangle_{V_j,U_j}$。另外的 $t$ 个粒子 $\left(V_1,V_2^{'},\cdots,V_{j-1}^{'},V_j,U_{j+1},\cdots,U_t\right)$ 坍塌到

$$\left|\psi\left(v_1+\sum_{r=1}^{j}s_r,v_2^{'},\cdots,v_{j-1}^{'},v_j^{'},u_{j+1},\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},\cdots,V_{j-1}^{'},V_j^{'},U_{j+1},\cdots,U_t}。$$

此时的混合系统为 $\left|\Psi_j\right\rangle$：

$$\left|\Psi_j\right\rangle=\left|\psi\left(v_1+\sum_{r=1}^{j-1}s_r,v_2^{'},\cdots,v_{j-1}^{'},u_j,\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},\cdots,V_{j-1}^{'},U_j,\cdots,U_t}\otimes\left|\psi\left(v_j,v_j^{'}\right)\right\rangle_{V_j,V_j^{'}}$$

$$=\frac{1}{d}\sum_{l_j,k_j=0}^{d-1}\zeta^{-l_jk_j}\left|\psi\left(v_1+\sum_{r=1}^{j-1}s_r+k_j,v_2^{'},\cdots,v_{j-1}^{'},v_j^{'}+l_j,u_{j+1},\cdots,u_t\right)\right\rangle_{V_1,V_2^{'},\cdots,V_{j-1}^{'},V_j^{'},U_{j+1},\cdots,U_t}\otimes\left|\psi\left(v_j-k_j,u_j-l_j\right)\right\rangle_{V_j,U_j}。\tag{8}$$

d）当最后一个参与者 $Bob_t$ 使用投影算子 $\left|\psi\left(v_t-s_t,u_t\right)\right\rangle\left\langle\psi\left(v_t-s_t,u_t\right)\right|$ 对持有的粒子 $\left(V_t,U_t\right)$ 进行投影测量，测量的结果为 $\left|\psi\left(v_t-s_t,u_t\right)\right\rangle_{V_t,U_t}$。另外的 $t$ 个粒子 $\left(V_1,V_2^{'},\cdots,V_{t-1}^{'},V_t^{'}\right)$ 坍塌到 $\left|\psi\left(v_1+\sum_{r=1}^{t}s_r,v_2^{'},\cdots,v_{t-1}^{'},v_t^{'}\right)\right\rangle_{V_1,V_2^{'},\cdots,V_{t-1}^{'},V_t^{'}}$。当所有参与者投影测量完成，复合系统产生的纠缠交换如图 4 所示。

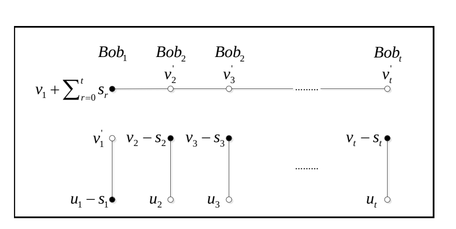



图 4　粒子 $\left(V_t,U_t\right)$ 投影测量后的纠缠交换结果

### 1.4　秘密重建阶段

在本阶段，重建者 $Bob_1$ 持有的 $V_1$ 粒子，恢复出共享的秘密，并进行 hash 值比对，判断是否存在不诚实的参与者。

a） $Bob_1$ 对持有的粒子 $V_1$ 使用测量基 $\{|J_q\rangle \mid q=0,1,\cdots,d-1\}$ 进行测量，其中 $|J_q\rangle=\frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}\zeta^{pq}|p\rangle$。测量结果应为 $|J_{q'}\rangle$，其中，$q'=v_1+\sum_{r=1}^{t}s_r$。这是因为，在第 1.3 章第 d）步，当 $Bob_t$ 对粒子 $(V_t,U_t)$ 测量之后，坍塌的 $t$ 个粒子 $(V_1,V_2',\cdots,V_{t-1}',V_t')$ 可表示为

$$\left|\psi\left(v_1+\sum_{r=1}^{t}s_r,v_2',\cdots,v_{t-1}',v_t'\right)\right\rangle_{V_1,V_2',\cdots,V_{t-1}',V_t'}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{\left(v_1+\sum_{r=1}^{t}s_r\right)q}|q\rangle_{V1}|q+v_2'\rangle_{V_2'}|q+v_3'\rangle_{V_3'}\cdots|q+v_t'\rangle_{V_t'} \tag{9}$$

b）已知测量结果 $|J_{q'}\rangle$ 和 $v_1$ 的值，$Bob_1$ 能计算出 $\sum_{r=1}^{t}s_r$ 的值。进一步，$Bob_1$ 计算 $hash\left(\sum_{r=1}^{t}s_r\right)$，并验证等式 $hash\left(\sum_{r=1}^{t}s_r\right)=hash(a_0)$。如果这个等式成立，他就和其他参与者共享这个秘密消息；否则，他认为至少存在一个不诚实的参与者，进而结束此次秘密重建过程，开始新一轮的重建过程。

## 2　正确性证明

$$\begin{aligned}&|\psi(u_1,u_2)\rangle_{1,2}\otimes|\psi(v_1,v_2)\rangle_{3,4}\\&=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{qu_1}|q\rangle_1|q+u_2\rangle_2\otimes\frac{1}{\sqrt{d}}\sum_{q'=0}^{d-1}\zeta^{q'v_1}|q'\rangle_3|q'+v_2\rangle_4\\&=\frac{1}{d}\sum_{q,q'}\zeta^{qu_1+q'v_1}|q\rangle_1|q'+v_2\rangle_4|q'\rangle_3|q+u_2\rangle_2\\&=\frac{1}{d^2}\sum_{q,q',p,p'}\zeta^{qu_1+q'v_1}\zeta^{-qp-q'p'}|\psi(p,q'+v_2-q)\rangle_{1,4}|\psi(p',q+u_2-q')\rangle_{3,2}\end{aligned} \tag{10}$$

令 $q'-q=l$，根据 $\frac{1}{d}\sum_{q=0}^{d-1}\zeta^{qm}=\delta(m,0)$，式(10)可写为

$$|\psi(u_1,u_2)\rangle_{1,2}\otimes|\psi(v_1,v_2)\rangle_{3,4}=$$

$$\frac{1}{d}\sum_{k,l}\zeta^{-kl}|\psi(u_1+k,v_2+l)\rangle_{1,4}\otimes|\psi(v_1-k,u_2-l)\rangle_{3,2} \tag{11}$$

由于在粒子 2 到粒子 $t$ 之间，多粒子纠缠态的粒子以及粒子的标签之间的交换是对应的，即

$$|\psi(u_1,\cdots,u_k,\cdots,u_l,\cdots,u_t)\rangle_{1,\cdots,k,\cdots,l,\cdots,t}=$$

$$|\psi(u_1,\cdots,u_l,\cdots,u_k,\cdots,u_t)\rangle_{1,\cdots,l,\cdots,k,\cdots,t}, \tag{12}$$

由式子(11)(12)可得

$$\begin{aligned}&|\psi(u_1,u_2,\cdots,u_t)\rangle_{1,2,\cdots,t}\otimes|\psi(v,v')\rangle_{V,V'}\\&=\frac{1}{d}\sum_{k,l}\zeta^{-kl}|\psi(v+k,u_2-l,u_3-l,\cdots,u_t-l)\rangle_{V,2,3,\cdots,t}\otimes\\&\qquad|\psi(u_1-k,v'+l)\rangle_{1,V'},\end{aligned} \tag{13}$$

$$\begin{aligned}&|\psi(u_1,u_2,\cdots,u_t)\rangle_{1,2,\cdots,t}\otimes|\psi(v,v')\rangle_{V,V'}\\&=\frac{1}{d}\sum_{k,l}\zeta^{-kl}|\psi(u_1+k,u_2,u_3,\cdots,v'+l,\cdots,u_t)\rangle_{1,2,\cdots,V',\cdots,t}\otimes\\&\qquad|\psi(v-k,u_m-l)\rangle_{V,m},\end{aligned} \tag{14}$$

式(6)由式(13)得出，式(7)(8)由式(14)得出。

## 3　安全性分析

### 3.1　截获-重发攻击

假设 Eve 是一个不诚实的内部参与者或者是外部窃听者，她截获第 1.2 章第 d）步中从 $Bob_1$ 发往 $Bob_j$ 的任意一个粒子 $u_j\ (j=2,3,...,t)$，然后使用测量基 $\{|0\rangle,|1\rangle,...,|d-1\rangle\}$ 去测量这个粒子。她有 $1/d$ 的概率成功获得 $u_j+q$ 的值，其中 $q\in\{0,1,...,d-1\}$。最后她制备一个一样的粒子重放给参与者 $Bob_j$。不过，她的测量结果 $u_j+q$ 并没有关于份额 $f(x_j)$ 和影子 $s_j$ 的任何信息。因此，Eve 的截获-测量-重发攻击不能获得任何有用的信息。

### 3.2　纠缠-测量攻击

假设 Eve 截获了第 1.2 章第 d）步中从 $Bob_1$ 发往 $Bob_j$ 的所有 $t-1$ 粒子 $\{U_2,U_3,\cdots,U_t\}$，然后她制备 $t-1$ 个辅助粒子 $\{|e_2\rangle,|e_3\rangle,\cdots,|e_t\rangle\}$。对于 $2t-1$ 个粒子组成的复合系统，Eve 以粒子 $U_j\ (j=2,3,...,t)$ 为控制粒子，以辅助粒子 $|e_j\rangle$ 为目标粒子分别进行 $d$ 维 $R_c$ 门操作，将得到

$$|\varphi_3\rangle=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\zeta^{qu_1}|q\rangle|u_2+q\rangle|u_3+q\rangle\cdots|u_t+q\rangle$$

$$|u_2+q+e_2\rangle|u_3+q+e_3\rangle\cdots|u_t+q+e_t\rangle。 \tag{15}$$

由 $|\varphi_3\rangle$ 可知，当 Eve 对 $|u_j+q+e_j\rangle$ 进行测量之后，已知 $|e_j\rangle(j=2,3,...,t)$ 的值，Eve 能得到 $u_j+q$ 的值，其中 $q\in\{0,1,...,d-1\}$。但是结果 $u_j+q$ 中并没有关于秘密份额 $f(x_j)$ 和秘密影子 $s_j$ 的任何信息。因此，Eve 的纠缠-测量攻击也不能获得任何有用的信息。

### 3.3　合谋攻击

在第 1.4 章的秘密重建过程中，假定在 $t$ 个参与者中，除了重建者 $Bob_1$ 是诚实的，其他参与者 $\{Bob_2,Bob_3,\cdots,Bob_t\}$ 都不诚实。当这 $t$-1 个参与者一起合谋，他们拿出自己持有的秘密影

子计算出这些影子的总和 $\sum_{j=2}^{t} s_j$，但他们并不知道 $Bob_1$ 的的秘密影子 $s_1$，也不能计算出最终的结果 $\sum_{j=1}^{t} s_j$。所以 $t$-1 个参与者 $\{Bob_2, Bob_3, \cdots, Bob_t\}$ 的合谋攻击失败。

### 3.4　伪造攻击

在第 1.3 章中，每个参与者对持有的粒子执行投影测量，假设有一个不诚实的参与者 $Bob_f$，他使用一个伪造的秘密影子 $s_f^*$ 代替真实的秘密影子 $s_f$，生成投影测量算子 $\left|\psi\left(v_f - s_f^*, u_f\right)\right\rangle\left\langle\psi\left(v_f - s_f^*, u_f\right)\right|$，其中，$s_f^* \neq s_f$。进一步，他使用该算子对持有的粒子 $\left(V_f, U_f\right)$ 执行投影测量。当所有参与者测量完毕，重建者 $Bob_1$ 将得到 $v_1 + s_1 + \cdots + s_f^* + \cdots + s_t$。当重建者 $Bob_1$ 验证等式 $hash\left(s_1 + \cdots + s_f^* + \cdots + s_t\right) = hash\left(a_0\right)$ 时，发现等式不成立，于是他认为在所有参与者中至少存在一个参与者拿出的是伪造的秘密份额或秘密影子。$Bob_1$ 取消本次重建过程，$Bob_f$ 的伪造攻击失败。

## 4　性能比较

由于提出的方案和方案[9]给出了秘密份额和影子的产生过程，而方案[6]和方案[13]并没有提及，为了更公平地比较，四个方案都不考虑秘密份额和影子的产生过程的开销。由于提出的方案用 $H_d$ 门和 $R_c$ 来制备多粒子纠缠态，而方案[6]和方案[13]没有提及多粒子纠缠态的制备过程，方案[9]也没有给出 $t$ 对 EPR 对的制备过程，所以 4 个方案比较时也不考虑制备纠缠态的开销。将提出的方案与其他 3 个文献的方案[6, 9, 13]从门限类型、空间维度、酉操作+$QFT$ 的次数、测量的次数、hash 运算的次数、信息效率六个方面进行比较，如表 1 所示。

表 1　4 个方案的比较

| 性能 | 方案 [6] | 方案[9] | 方案 [13] | 提出的方案 |
|---|---|---|---|---|
| 门限类型 | $(n,n)$ | $(t,n)$ | $(n,n)$ | $(t,n)$ |
| 空间维度 | $d$ | 2 | $d$ | $d$ |
| 酉操作+ $QFT$ 的次数 | $nU_{\alpha,0} + nQFT$ | $t(2t-1)U_{\alpha,\beta}$ | $NU_{0,\beta} + \left(N - C_1\right)\left(n+1\right)H_d$ | 0 |
| 测量的次数 | $n$ | $t$ | $N\left(n+1\right)$ | $t+1$ |
| hash 运算的次数 | | | | 2 |
| 信息效率 | $\frac{1}{2n}$ | $\frac{\lceil \log_2 d \rceil}{3tk + 2k + \lceil \log_2 d \rceil}$ | $\frac{1}{2N\left(n+1\right)}$ | $\frac{1}{3t}$ |

从表 1 可以看出，在门限方面，提出的方案和方案[9]都是 $(t,n)$ 门限方案，另外两种方案是 $(n,n)$ 门限方案。在 Hilbert 空间维度方面，方案[9]是 2 维方案，其他方案都是 $d\,(d>2)$ 维方案。在 4 个方案中，只有提出的方案是 $d$ 维 $(t,n)$ 门限方案。

在酉操作+$QFT$ 的次数方面，在方案[6]中，$n$ 个参与者先分别使用傅里叶变换 $(QFT)$ 对自己的粒子作变换，再分别使用 $U_{\alpha,0}$ 变换将自己的秘密份额加入到量子态中，该方案酉操作+$QFT$ 的次数为 $nU_{\alpha,0} + nQFT$。在方案[9]中，分发者先把 $Y'$ 序列发给 $Bob_1$，每一个参与者 $Bob_r$ 对来自于上一个参与者 $Bob_{r-1}$ 发给他的 $Y'$ 序列执行酉操作 $U_{\alpha,\beta}$。最后一个参与者 $Bob_t$ 对从 $Bob_{t-1}$ 收到的 $Y'$ 序列执行酉操作 $U = U_{B_1} U_{B_2} \cdots U_{B_t}$，没有执行 $QFT$ 操作。该方案酉操作+$QFT$ 的次数为 $t\left(2t-1\right)U_{\alpha,\beta}$。在方案[13]中，Alice 制备了 $N$ 对 $(n+1)$ 粒子的纠缠对，并将每个纠缠对中的第一粒子进行了 $U_{0,\beta}$ 操作，在选取 $C_1$ 个纠缠对进行窃听检测后，对剩余 $N - C_1$ 个纠缠对的每个粒子进行了哈达门变换 $H_d$。$QFT$ 另一种表示法是 $d$ 维哈达门变换 $H_d$，所以该方案酉操作+$QFT$ 的次数为 $NU_{0,\beta} + \left(N - C_1\right)\left(n+1\right)H_d$。提出的方案没有执行酉操作和 $QFT$，这两种操作的次数为零。

在测量的次数方面，方案[13]测量次数最多，为 $N\left(n+1\right)$ 次。由于 $t \le n$，方案[9]和提出的方案的测量次数相当，且少于其他两种方案。在 hash 运算方面，提出的方案有 2 次，其他方案没有。与酉操作+$QFT$，测量操作相比，hash 运算所花费的开销要小得多。

信息效率计算公式为 $\eta = c/\left(q+b\right)$，这里 $c$ 为秘密消息的经典比特总数，$q$ 为制备粒子总数，$b$ 为经典信道交换的经典比特总数。提出的方案和其他三个文献[6，9，13]的方案都恢复了一个 $d$ 维的秘密消息（$\lceil \log_2 d \rceil$ bits），因此 $c$ 的值都为 $\lceil \log_2 d \rceil$。提出的方案第一轮制备了 $3t$ 个 $d$ 维粒子，且没有用经典信道传输经典比特，所以提出的方案的第一轮的信息效率为 $\eta = \frac{\lceil \log_2 d \rceil}{3t\lceil \log_2 d \rceil} = \frac{1}{3t}$。方案[6]需要制备 $n$ 个 $d$ 维粒子，且需要利用经典信道公布 $n$ 个 $d$ 维粒子的测量结果，因此方案[6]的信息效率为 $\eta = \frac{\lceil \log_2 d \rceil}{n\lceil \log_2 d \rceil + n\lceil \log_2 d \rceil} = \frac{1}{2n}$；方案[9]由于在秘密重构阶段，秘密份额的影子需要在量子信道中传输，为保证可抵抗窃听攻击，其使用了插入诱骗粒子进行窃听检测的方法，方

案[9]制备了 $m$ 个 EPR 粒子对，这里的 $2m=\lceil \log_2 d \rceil$，并需要进行 $(t+1)$ 窃听检测，制备的诱骗粒子总数为 $2k+(t-2)k$，而且经典信道里需要交换诱骗粒子的位置信息和测量结果信息共 $2k(t+1)$ bits，因此方案[9]的信息效率为 $\eta=\frac{\lceil \log_2 d \rceil}{2k+(t-2)k+\lceil \log_2 d \rceil+2k(t+1)}=\frac{\lceil \log_2 d \rceil}{3tk+2k+\lceil \log_2 d \rceil}$，这里 $k \ge 1$。方案[13]需要制备 $N$ 对 $n+1$ 粒子的 $d$ 维纠缠态，并且最终恢复秘密后，所有的粒子都被测量完了，而且测量结果都需要通过经典信道进行公布，所以需要交换 $N(n+1)\lceil \log 2^d \rceil$ bits 信息，因此方案[13]的信息效率为 $\eta=\frac{\lceil \log_2 d \rceil}{N(n+1)\lceil \log_2 d \rceil+N(n+1)\lceil \log_2 d \rceil}=\frac{1}{2N(n+1)}$。而且，提出的方案每一轮秘密共享只消耗 $t$ 个 $d$ 维粒子，秘密恢复后剩下的 $t$ 对 2 粒子纠缠态可以在下一轮继续使用，并在以后每一轮都可以继续使用。因此，从第二轮开始，提出的方案的信息效率将变为 $\eta=\frac{\lceil \log_2 d \rceil}{t\lceil \log_2 d \rceil}=\frac{1}{t}$。而方案[6, 9, 13]中制备的粒子无法继续使用，全部被消耗了，下一轮需重新制备，因此方案[6, 9, 13]的信息效率在第二轮后是不变的。很明显，提出的方案的信息效率较高。

## 5　结束语

提出的以 $d$ 维纠缠交换为技术手段，提出了一个 $(t,n)$ 门限量子秘密共享方案。安全性分析可知，提出的方案能抵抗截获-重发攻击、纠缠-测量攻击、合谋攻击和伪造攻击。它应用纠缠交换实现隐形传输，份额没有在量子信道中传输，比其他现有类似方案具有更强的安全性。性能比较分析表明，提出的方案是 $d$ 维 $(t,n)$ 门限方案，相比其他 2 维或 $(n,n)$ 门限方案，提出的方案具有更好的灵活性、实用性和普适性。由于提出的方案没有执行酉操作和 $QFT$，总的计算和测量所花费的开销在现有类似方案中是最低的。后期的研究是探寻如何将提出的 $d$ 维 $(t,n)$ 门限量子秘密共享应用于量子群通信环境中，设计量子门限签名，量子门限加密等方案。

## 参考文献：


[1] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59 (3): 1829-1834.

[2] Wang wenhua, Cao Huaixin. An improved multiparty quantum secret sharing with bell states and Bell measurement [J]. International Journal of Theoretical Physics, 2013, 52 (6): 2099-2111.

[3] Qin Huawang, Dai Yuewei. Efficient quantum secret sharing [J]. Quantum Information Processing, 2016, 15 (5): 2091-2100.

[4] Tan Xiaoqing, Jiang Lianxia. Improved three-party quantum secret sharing based on Bell states [J]. International Journal of Theoretical Physics, 2013, 52 (10): 3577-3585.

[5] Zhang Zhanjun, Man Zhongxiao. Multiparty quantum secret sharing based on entanglement swapping [J]. Physical Review A, 2005, 72 (2) .

[6] Yang Wei, Huang Liusheng, Shi Runhua, et al. Secret sharing based on quantum Fourier transform [J]. Quantum Information Processing, 2013, 12 (7): 2465-2474.

[7] Tavakoli A, Herbauts I, Żukowski M, et al. Secret sharing with a single d-level quantum system [J]. Physical Review A, 2015, 92 (3) .

[8] Yang Yuguang, Wen Qiaoyan. Circular threshold quantum secret sharing [J]. Chinese Physics B, 2008, 17 (2): 419-423.

[9] Li Baokui, Yang Yuguang, Wen Qiaoyan. Threshold quantum secret sharing of secure direct communication [J]. Chinese Physics Letters, 2009, 26 (1): 21-24.

[10] Cleve R, Gottesman D, Lo H K. How to share a quantum secret [J]. Physical Review Letters, 1999, 83 (3): 648-651.

[11] Guo Ying, Huang Dazu, Zeng Guihua, et al. Multiparty quantum secret sharing of quantum states using entanglement states [J]. Chinese Physics Letters, 2008, 25 (1): 16-19.

[12] Qin Huawang, Zhu Xiaohua, Dai Yuewei. (t, n) threshold quantum secret sharing using the phase shift operation [J]. Quantum Information Processing, 2015, 14 (8): 1-8.

[13] Xiao Heling, Gao Jingliang. Multi-party d-level quantum secret sharing scheme [J]. International Journal of Theoretical Physics, 2013, 52 (6): 2075-2082.

[14] Huang Dazu, Chen Zhigang, Guo Ying. Multiparty quantum secret sharing using quantum fourier transform [J]. Communications in Theoretical Physics, 2009, 51 (2): 51-221.

[15] Qin Huawang, Dai Yuewei. Proactive quantum secret sharing [J]. Quantum Information Processing, 2015, 14 (11): 4237-4244.

[16] Song Tingting, Wen Qiaoyan, Qin Sujuan, et al. The general theory of three-party quantum secret sharing protocols over phase-damping channels [J]. Quantum Information Processing, 2013, 12 (10): 3291-3304.

[17] Dehkordi M H, Fattahi E. Threshold quantum secret sharing between multiparty and multiparty using Greenberger-Horne-Zeilinger state [J]. Quantum Information Processing, 2013, 12 (2): 1299-1306.

[18] Yang Yuguang, Jia Xin, Wang Hongyang, et al. Verifiable quantum (k, n) -threshold secret sharing [J]. International Journal of Theoretical Physics, 2011, 50 (3): 792-798.

[19] Deng Fuguo, Li Xihan, Zhou Hongyu. Efficient high-capacity quantum secret sharing with two-photon entanglement [J]. Physics Letters A, 2006, 372 (12): 1957-1962.

[20] Song Xiuli, Liu Yanbing. Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing [J]. Quantum Information Processing, 2016, 15 (2): 851-868.

[21] Karimipour V, Bahraminasab A, Bagherinezhad S. Entanglement swapping of generalized cat states and secret sharing [J]. Physical Review A, 2001, 65 (4): 579-579.